+ where the company's name-linked files are kept;

+ who manages them and is responsible for training staff on data security procedures;

+ whether there is a companywide policy on how frequently to review records to ensure they are up to date;

+ whether there is an agreed maximum period before records are destroyed;

+ whether name-linked files are registered with the appropriate authorities in each country where this is necessary;

+ whether the company's export of data complies with national law and has the appropriate national approval;

+ whether by complying with US law on monitoring the employment of minority ethnic groups the company data files will conflict with any European national laws on compiling sensitive data on racial or ethnic groups.

PRIVACY LAWS AND FINANCIAL INFORMATION

The introduction of data protection legislation will affect two main areas of financial information:

+ data on individuals' bank accounts, insurance policies etc.,

+ data on individuals' credit worthiness.

In the first case, the individual knows that he has a bank account or an insurance policy and which financial institution he deals with. He has a contractural relationship and if he wishes to seek access to his record to exercise his data protection rights, he knows where he must make his request.

The second case is quite different in data protection terms because in this instance the individual data subject does not normally have a contractural relationship with the data owner. The credit information company can collect information on an individual and supply it to a third party without the data subject being aware of the process. The data subject may be aware of the data collection process only when he seeks and is refused credit or is granted credit at unfavorable terms.

For this reason credit information has been regulated by separate laws in some countries, for example, Sweden and the UK. Indeed in the UK, the Consumer Credit Act of 1974, giving individuals a right of access to their credit information records, was passed a

decade before the Data Protection Act in 1984.

Examples of the impact of data protection laws on credit information operations may be drawn from across Europe:

+ Complaints. In several countries, such as Denmark and the UK, the second highest category of complaints to data protection authorities, after direct marketing, concerns credit information. In the UK Data Protection Registrar's second annual report published in July this year, he states that the problem is the relevance of information held to provide credit references. "Broadly, the concern is about the supply of information not apparently directly related to the individual requesting credit."

+ Investigations. The volume of complaints often leads to the data authority making a special study of this sector. One chapter of the recently published annual report from France's data protection authority reported on its work in this area.

+ Registration. If a country has a detailed and simplified data protection registration form, like France, credit information comes into the detailed category.

+ Licensing. If a country, like Denmark, has a data protection licensing system for certain categories of business, then credit information bureaus will be included.

+ Shutting down an operation. Among the few examples from around Europe where a company has had its operation shut down is a credit information company in Norway.

+ Exporting name-linked data. In Germany, The Land (provincial) officials responsible for enforcing data protection legislation for companies meet three or four times a year to discuss common problems so they can implement consistent policies. On one occasion, they discussed how the German law should be applied to the export of credit information.

Their starting point was that the export of credit information from Germany is illegal if a domestic transfer would be under the same circumstances, or if there is a clear lack of data protection in the country receiving the data. They then considered whether credit information should be exported to an inquiry office in Austria, which does have a comprehensive data protection law. The owner of the data in this case was SCHUFA, the Protective Association for General Credit Precautions. It has a data bank on about 21 million people and stores information on individuals' loans, methods of repayment and, for example, whether the repayment schedule has been met. The Land officials took the decision to permit data to be sent to an inquiry office in Austria that accepted requests for individuals' data stored in Germany. Although an inquiry about an individual was allowed, it would not be permitted to answer a request for the creditworthiness of a large group.